CLAIMS

What is claimed is:

1. In a wireless network environment comprising at least one authorized access point connected to a wired computer network, a method for detecting whether a rogue access point is connected to the wired computer network, comprising

detecting a rogue access point,

identifying at least one authorized access point that neighbors the rogue access point;

selecting an authorized access point from the at least one authorized access point in the identifying step;

establishing a wireless connection between the selected authorized access point and the rogue access point;

wirelessly transmitting a rogue location discovery packet from the selected authorized access point to the rogue access point, wherein the rogue location discovery packet is addressed to a network device connected to the computer network;

monitoring for receipt of the rogue location discovery packet at the network device.

2. The method of claim 1 wherein the network device is the authorized access point.

3. The method of claim 1 wherein the network device is a central control element.

4. The method of claim 1 further comprising

applying at least one rogue containment method, if the rogue location discovery packet is received at the network device.

5. The method of claim 1 further comprising

reporting the detected rogue access point, if the rogue location discovery packet is not received at the network device within a threshold period of time.

6. The method of claim 1, wherein the wired computer network is implemented by at least one network device operative to switch or route data units between devices connected thereto, the data units including a source address and a destination address, wherein the at least one network device comprises at least two ports to which other devices connect, and wherein the at least one network device is operative to store the source addresses of the data units encountered at the ports of the at least one network device, and wherein the method comprises

if the rogue location discovery packet is not received at the network device within a threshold period of time, then

determining the address of at least one rogue client associated with the rogue access point; and

identifying the port to which the rogue access point is connected by querying, using the addresses of the at least one rogue client in the determining step, the at least one network device for the port at which data units sourced from the at least one rogue client were encountered.

7. The method of claim 6 further comprising

disabling the identified port.

8. The method of claim 6 further comprising

locating the edge port, if more than one network device responds in the polling step.

9. The method of claim 6 wherein the at least one network device is an Ethernet switch.

10. In a wireless network environment comprising at least one authorized access point connected to a wired computer network, the wired computer network including dynamic network address assignment functionality, a method for detecting whether a rogue access point is connected to the wired computer network, comprising

detecting a rogue access point,

identifying at least one authorized access point that neighbors the rogue access point;

selecting an authorized access point from the at least one authorized access point in the identifying step;

establishing a wireless connection between the selected authorized access point and the rogue access point;

obtaining a dynamic computer network address for the selected authorized access point;

wirelessly transmitting a rogue location discovery packet from the selected authorized access point to the rogue access point, wherein the rogue location discovery packet is logically addressed to a network device connected to the computer network;

monitoring for receipt of the rogue location discovery packet at the network device.

11. The method of claim 10 wherein the network device is the authorized access point.

12. The method of claim 10 wherein the network device is a central control element.

13. The method of claim 10 further comprising

applying at least one rogue containment method, if the rogue location discovery packet is received at the network device.

14. The method of claim 10 further comprising

reporting the detected rogue access point, if the rogue location discovery packet is not received at the network device within a threshold period of time.

15. The method of claim 10 wherein the rogue location discovery packet includes a digital signature.

16. The method of claim 10 further comprising comparing the obtained dynamic network address to the network address of the network device to determine whether the network device and the rogue access point are connected to the same subnet.

17. The method of claim 16 further comprising

transmitting an Address Resolution Protocol request to resolve the link layer address of a gateway node, if the network device and the rogue access point are on different subnets; and

setting the link layer destination address of the rogue location discovery packet to the link layer address in the response to the Address Resolution Protocol request.

18. In a wireless network environment comprising at least one authorized access point connected to a wired computer network, the wired computer network including dynamic network address assignment functionality, a method for detecting whether a rogue access point is connected to the wired computer network, comprising

detecting a rogue access point,

observing at least one data frame including a logical network address of a wireless client associated with the rogue access point;

selecting a logical network address identified in the observing step;

identifying at least one authorized access point that neighbors the rogue access point;

selecting an authorized access point from the at least one authorized access point in the identifying step;

establishing a wireless connection between the selected authorized access point and the rogue access point;

wirelessly transmitting a rogue location discovery packet from the selected authorized access point to the rogue access point, wherein the rogue location discovery packet is logically addressed to a network device connected to the computer network; and wherein the source address of the rogue location discovery packet is set to the logical network address of the selected wireless client; and

monitoring for receipt of the rogue location discovery packet at the network device.

19. In a computer network environment comprising a wired computer network implemented by at least one network device operative to switch or route data units between devices connected thereto, the data units including a source address and a destination address, wherein the at least one network device comprises at least two ports to which other devices connect, and wherein the at least one network device is operative to store the source addresses of the data units encountered at the ports of the at least one network device, a method for network location of a rogue access point, comprising

detecting a rogue access point,

determining the address of at least one rogue client associated with the rogue access point; and

querying, using the addresses of the at least one rogue client in the determining step, the at least one network device for the port at which data units sourced from the at least one rogue client were encountered.

20. The method of claim 19 further comprising

if the at least one network device responds with an identified port, disabling the identified port.

21. The method of claim 19 further comprising

locating the edge port, if more than one network device responds in the polling step.

22. The method of claim 19 wherein the at least one network device is an Ethernet switch.

23. A wireless network system facilitating network location of rogue systems, comprising

a plurality of access elements for wireless communication with at least one remote client element and for communication with a central control element;

a central control element for supervising at least one of said access elements, wherein the central control element is operative to manage and control the wireless connections between the access elements and corresponding remote client elements; the central control element including at least one network interface operatively connected to a wired computer network; and

wherein the access elements are each operative to:

establish and maintain, in an access point mode, wireless connections with remote client elements; and

wherein the access elements, under control of the central control element are further operative to:

establish a wireless connection to a detected rogue access point;

transmit a rogue location discovery packet to the detected rogue access point, wherein the destination address of the rogue location discovery packet is set to the central control element;

and wherein the central control element is operative to:

monitor for receipt of rogue location discovery packets on the network interface.

24. The system of claim 23 wherein the rogue location discovery packet is sourced from the central control element to the access element.

25. The system of claim 23 wherein the access element, under control of the central control element, is further operative to obtain a dynamic logical network address.

26. The system of claim 23 wherein the central control element is further operative to apply at least one rogue containment method, if the rogue location discovery packet is received at the network device.

27. The system of claim 23 wherein the central control element is further operative to report the detected rogue access point, if the rogue location discovery packet is not received at the network device within a threshold period of time.

28. The system of claim 23 wherein the access elements are further operative to

switch to a scanning mode for a scanning period at a scanning interval to detect wireless traffic,

record scan data characterizing the detected wireless traffic, and

transmit the scan data to the central control element; and

wherein the central control element is operative to

process the scan data against information relating to known access elements to identify rogue access points,

to contain the detected rogue access point(s).

29. The system of claim 23 wherein the central control element is operative to

establish a tunnel with access elements for transmission of wireless traffic associated with corresponding remote client elements, and

bridge network traffic between the computer network and a remote client element through a tunnel with a corresponding access element.